ATIS-0100033

Multi-Layer Coordination in All-IP Networks

Technical Report

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

> NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.

ATIS-0100033, *Multi-Layer Coordination in All-IP Networks*

Is an ATIS Standard developed by the **Quality of Service (QoS) Working Group** of the **ATIS Network Performance, Reliability, and Quality of Service Committee (PRQC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Printed in the United States of America.

ATIS-0100033

Technical Report on

Multi-Layer Coordination in All-IP Networks

Alliance for Telecommunications Industry Solutions

Approved May, 2011

Abstract

Service availability has received strong attention in ATIS PRQC in terms of metric definitions as well as measurement methodologies. This Technical Report (TR) addresses the issue of multi-layer coordination in All-IP networks. The term "All-IP" is a broad term to describe some key architectural evolutions in telecommunication core and access networks that are being deployed. The general idea behind it is that one network transports all information and services (voice, data, and all sorts of media such as video) by encapsulating these into packets, like it is on the Internet.

FOREWORD

The Performance Reliability and Quality of Service (PRQC) develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PRQC Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PRQC, which is responsible for the development of this Technical Report, had the following members:

P. Tarapore, PRQC Chair (AT&T)
M. Niebert, PRQC Vice-Chair (Telcordia)
H. Pant, Technical Editor (Huawei)
C.A. Underkoffler, ATIS Chief Editor

The PRQC Quality of Service (QoS) Working Group, which was responsible for the development of this document, had the following members:

Active Participants:

K. Biholar	M. Linnell
J. Colombo	S. Makris
C. Dvorak	A. Nguyen
E. Geelen	H. Pant
X. Gong	P. Tarapore
O. Lima	W. Xiangping

TABLE OF CONTENTS

TABLE OF FIGURES

Technical Report on

Multi-Layer Coordination in All-IP Networks

1 Scope & Purpose

Service availability has received strong attention in ATIS PRQC in terms of metric definitions as well as measurement methodologies. This Technical Report (TR) addresses the issue of multi-layer coordination in All-IP networks. The term "All-IP" is a broad term to describe some key architectural evolutions in telecommunication core and access networks that are being deployed. The general idea behind it is that one network transports all information and services (voice, data, and all sorts of media such as video) by encapsulating these into packets, like it is on the Internet.

The move to All-IP is a recognized technology trend in telecommunication networks. Many operators have finished the transition from traditional networks to All-IP networks or are on the way. However, All-IP networks also introduce new challenges in the area of reliability and security.

Given an All-IP network, there are many fault detection and localization mechanisms deployed on different network layers. However, the consideration of coordination among network layers is generally lacking in early network design. This leads to challenges in network-level fault diagnosis. Additionally, a promised benefit of the new technology is standardization, implying that the All-IP networks will be multi-vendor networks. This fact creates an additional challenge for multi-layer network coordination because the failure modes and recovery strategies of one vendor are unlikely to be made transparent to a competitor. New work was also initiated in ITU-T Study Group 12 Question 17 on guidelines for common IP/MPLS/Ethernet service classes to support interconnection between providers.

Specifically, this TR discusses multi-layer coordination for All-IP networks. Multi-layer coordination is essential for failure detection and correction. It discusses a methodology that has been employed to address multi-layer coordination challenges in large service-provider networks. This methodology applies the failure mode and effects analysis (FMEA) concepts to networks [Xian-2010].

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards and technical reports are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Xian-2010] - W. Xiangping and H. Pant “FMEA of Multi Layer Coordination in All IP Network,” *IEEE Communication Quality & Reliaility*, June 2010.

[Deem-1999] - P. Deemester et al, “Resilience in Multi-Layer Networks,” *IEEE Communications Magazine*, August 1999.

[Zupa-2003] - J. Zupan & D. Medhi, “An Alarm Management Approach in the Management of Multi-Layered Networks”, *IPOM 2003*, IEEE.

[Maes-2002] - S. De Maesschalck, “Intelligent Optical Networking for Multilayer Survivability”, *IEEE Communications Magazine*, January 2002.

[Nrsc-1999] - NRSC < http://www.atis.org/NRSC/Docs/1999Rpt.PDF >.

[Nrsc-1993] - Fiber Optic Cable Dig-Ups: Causes and Cures, *Network reliability: A Report to the Nation*, Network Reliability Council, June 1993.[1]

[Nrsc-1996] - *Keeping the Network Alive and Well: Solving the Problem of Cable Dig-Ups*, ATIS Network Reliability Steering Committee, Facilities Solution Team, February 1996.[1]

[Nrsc-1997] - *Fixing Facility Outages: Building the Tools to Make it Happen*, ATIS Network Reliability Steering Committee Facilities Solution Team, November 1997.[1]

[Fcc-Nrc] - FCC's Network Reliability Council (NRC) *Network Reliability: A Report to the Nation*.[1]

[Tel-Glos] - ATIS Telecom Glossary, < http://www.atis.org/glossary/ >.

3 DEFINITIONS

3.1 Definitions

3.1.1 Degradation: Degradation means the connection is not broken, but a performance problem exists, such as, packet loss or delay exceeding the permissible threshold.

3.1.2 Interruption: Interruption means that the connection is broken and no information can be transferred along this connection.

3.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
AIS	Alarm Indication Signal
LOF	Loss of Frame
LOS	Loss of Signal
FMEA	Failure Mode and Effects Analysis
GMPLS	Generalized Multiprotocol Label Switching
KPI	Key Performance Indicators
OAM	Operations, Administration and Maintenance
IP	Internet Protocol
NE	Network Element
OLP	Optical Line Protection (card)
OpEx	Operations Expenditure
OTU	Optical Transponder Unit
POS	Packet Over SONET/SDH
PRBS	Pseudo Random Bit Signal
PSTN	Public Switched Telephone Network
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SONET	Synchronous Optical Network

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

TR	Technical Report
WDM	Wavelength Division Multiplexing

5 INTRODUCTION & RATIONALE

Recent years have seen a growth in All-IP networks. Video and content rich services are booming due to affordable broadband, multiplicity of smart devices, and video/multimedia applications. One consequence of this growth in All-IP supported real-time services is the increased demand for improvement in operations, administration, and maintenance (OAM) of the All-IP networks. Improved OAM has to speed-up failure identification, fault diagnosis, and service restoral as real time services are sensitive to network performance. The need for improved OAM has a business driver as well. It will reduce customer churn by reducing service down-time but with tight profit margins, service providers will appreciate reduction in maintenance cost as well.

A major challenge to improved OAM in All-IP networks is lack of coordination between the different layers of an All-IP network. This problem has also been observed in non-All-IP networks multi-layer networks. A 2-layer network with a base SDH layer and a client ATM layer provides an example of the kind of problems arising from lack of multi-layer coordination [Deem-1999]. In the example, the network is designed to recover at the lowest possible layer, as close to the failure as possible. However, due to inadequate design for multi-layer coordination, the SDH alarms initiated for recovery from a cable-cut are delayed. This leads the ATM layer to believe that the failure occurs on its layer, thus triggering ATM layer recovery. Since the network resources are dimensioned for SDH layer recovery, the situation will lead to network congestion and other undesired behavior.

An example of this lack of coordination in All-IP networks is failure to synchronize the hold-off timers. In the event of a failure, this lack of coordination between the layers can lead to race conditions. Different network layers resort to simultaneous restoration activity that lead to route flapping and network instability. As an extreme step to avoid such situations, the operator may turn off the resiliency mechanisms on a layer.

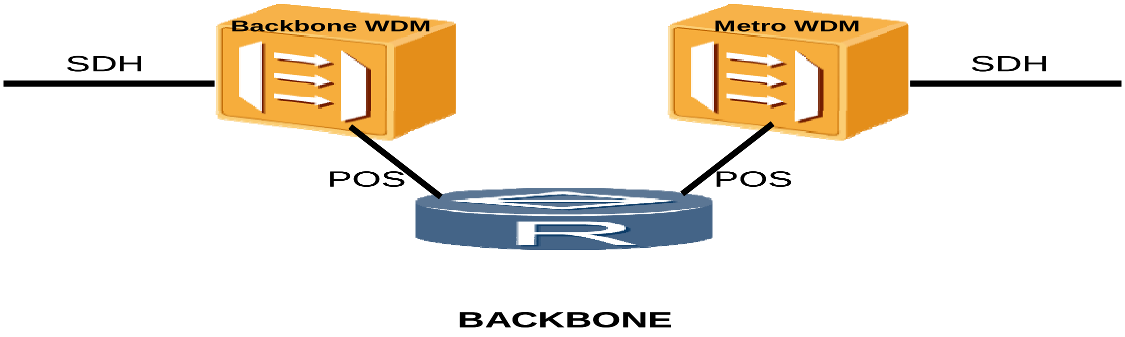


Figure 1a

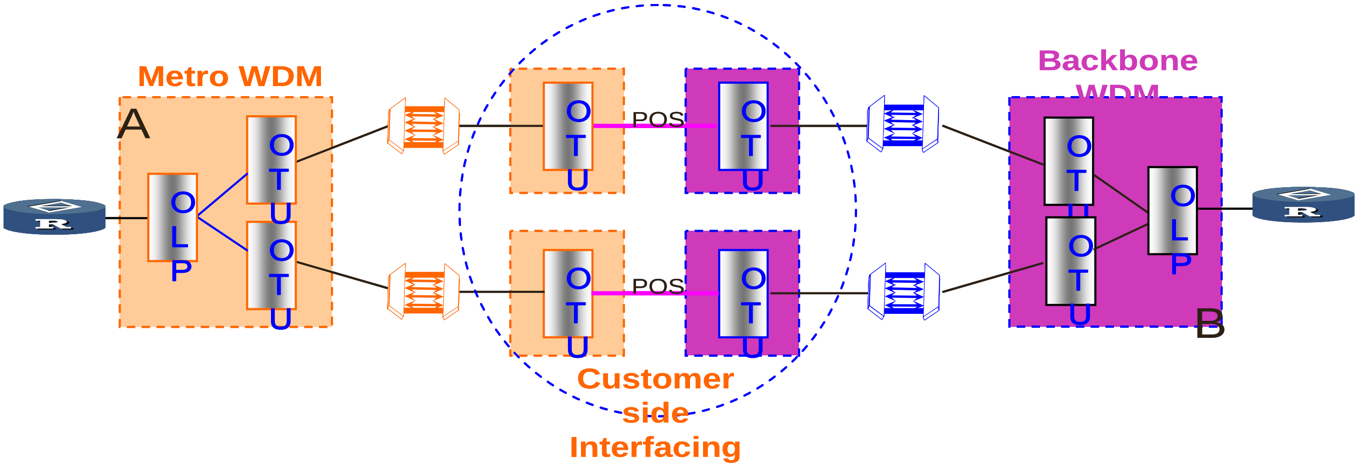


Figure 1b

Legend:
POS = Packet Over SONET/SDH
OLP = Optical Line Protection (card)
OTU = Optical Transponder Unit

Figure 1 - An Example of Lack of Coordination among Network Layers

Figure 1 provides an example of a failure scenario arising from unsynchronized hold-off timers. The network backbone, as shown in Figure 1a, consists of a metro Wavelength Division Multiplexer (WDM) assumes a metro WDM and a router. Thus, the metro WDM connects with the backbone WDM on Packet Over SONET/SDH (POS) interfaces. Figure 1b shows the relevant details on a simplified diagram. In the event of a failure (e.g., a fiber cut), the OLP at the optical layer is designed to ensure a hitless failover by detecting and switching over to a working path in less than 50 ms. However, the restoration time in an optical network may exceed 50 ms due to the processing latency in the POS interface. This will lead to re-convergence of the IP bearer layer, resulting in service(s) impairment.

There might be two corrective actions for this problem in case the network designer continues with the same backbone configuration. One is to improve the processing mechanism on the POS interfaces to ensure the restoration time of optical network be within 50 ms. Another one is to broaden the hold off timer on the IP bearer network. That is, the IP bearer network should wait a longer time thus allowing the optical network to restore.

Another issue in multi-layered network management is the lack of alarm correlation. For an overlay network, a fault can result in a chain reaction among the different network layers, leading to a set of alarms in each of the network layers. These alarms can be numerous and without a clear cause, which makes it difficult for the network operators to localize the fault in time. The problem and its relation to the survivability of networks are recognized and research solutions have been proposed to address automated alarm correlation in multi-layer networks [Zupa-2003].

Work is being done by vendors and network operators, to address the above problems. Standard bodies too have been active as evidenced by the GMPLS protocol which addresses the coordination between IP and optical by creating a single control plane that extends from IP at Layer 3 right down to the optical transport level at Layer 1. It thus improves network restoration capabilities and reduces operating expenses.

The objective of this contribution is to provide a tested solution as a methodology to improve the failure protection and alarming of multi-layer networks. The proposed methodology provides a detailed view of the network's protection mechanisms, alarms, and their interaction, thus leading to many benefits for network designers and operators.

This methodology will be of use for the network operators and service providers.

6 CHALLENGES FACING MULTI-LAYER NETWORK COORDINATION

Multi-layer coordination becomes an issue when a failure occurs on an All-IP telecommunications network. To address this issue, the reliability stakeholders need to understand the network's failure modes, the consequent failures, and the diagnostic and recovery processes triggered by each failure. For multi-layer coordination in All-IP networks, the alarming and protection strategies for the different layers cannot be designed in isolation. They have to be understood and designed in the context of end-to-end requirements for protection strategies while identifying the requirements for each of the layers that make up the multi-layer network. A well-designed network will ensure accurate fault localization to ensure network and service reliability, as well as to contain network operations cost.

The following list of questions summarizes the information that should be captured.

- What will be the impact of the failure linked to a failure mode on the different network layers and on the end-users' services?
- What protection mechanisms on different network layers will be triggered to deal with this failure? Implicit to this is the design question – in which layer of multi-layer network should the designers provide network recovery? In an IP over optical network, recoveries at the optical layer may be preferable for reasons of simplicity, size, and speed. However, not all failures can be recovered at the optical layer (e.g., an IP router failure) [Maes-2002].
- What are the trigger conditions for these protection mechanisms?
- What alarms will arise on different network layers?
- How do these alarms traverse the network layers?
- How are the alarms correlated to achieve the desired result of restoring service with minimum impact on end-customers?

7 MULTI-LAYER COORDINATION METHODOLOGY FOR ALL-IP NETWORK

The above list of questions is similar to the approach taken by the Failure Mode and Effects Analysis (FMEA) reliability engineering technique. FMEA has been used in the telecommunications industry to improve a system's reliability by analyzing and ultimately removing a system's failure modes. The aim of the FMEA is to take action in a prioritized order to eliminate failure modes and thus reduce failures in a system.

The network FMEA ensures multi-layer network coordination. As shown in Figure 2, the analytical structure of the FMEA for products can be used to define the steps for the network FMEA.

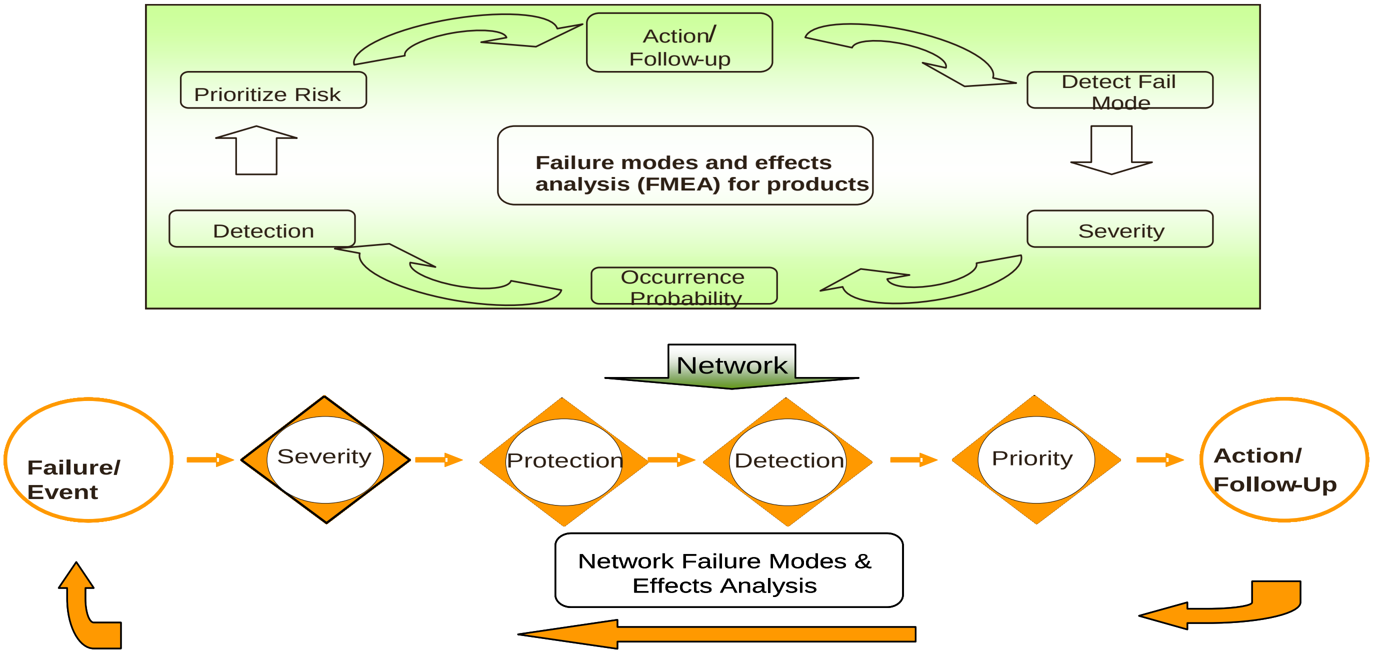


Figure 2 - From FMEA to Network FMEA

The steps in the Network FMEA are as follows[2]:

- **Failure Event**: Identify the failure events and their respective failure modes. Note that failure modes and consequent failures are usually identified during design but a failure event occurring in the field can point to a hitherto unidentified failure and its failure mode. The field failure may either be reported by the service subscriber or be identified by the network management system after analyzing the reported alarms.
- **Severity**: For each failure, this step identifies the failure's effect on the entire network, on the services (e.g., the number of services affected), and on the customers (e.g., number of customers affected for each service). Understanding these effects will enable the determination of a failure's severity. How exactly the effect on the service and on the network is translated into the failure's severity is beyond the scope of the TR.
- **Protection**: Identify protection mechanisms on each of the network layers. Details of how the network and service recovery may be affected in the event of failure can be obtained from the network design.
- **Detection**: Identify the alarms generated at each layer and gather information on the alarms that are triggered. The information includes details such as the trigger conditions for the alarms and how the alarms traverse through the layers.

[2] Note: The methodology assumes successful completion of preliminary steps that relate to defining the in-scope network and gathering information. These will be mentioned in the examples.

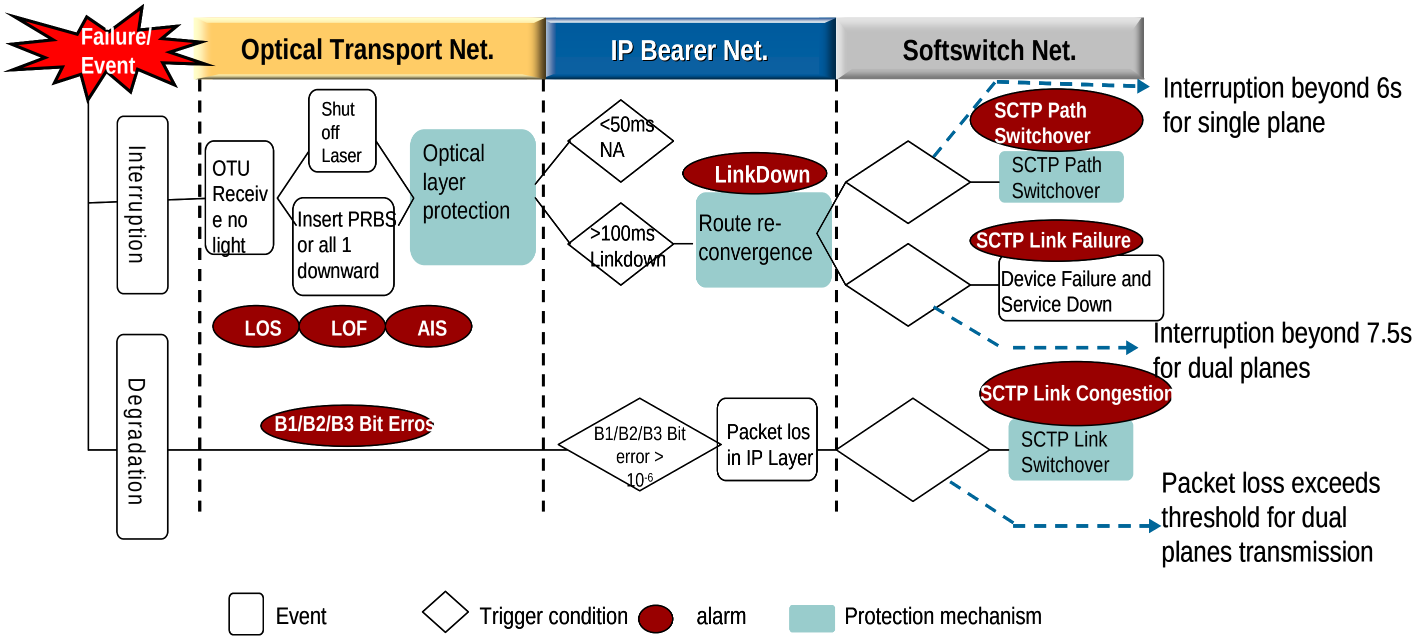
- **Priority**: Determine the failure's priority based on the chance of occurrence, the ease of detection and the severity. Knowing the priority is an aid to decision making. Failure modes that result in high priority failures will be rectified first.
- **Action & Follow-Up**: Develop solutions to rectify the failure mode and avoid similar problems in the future.

In the next section, examples are discussed that apply the methodology to actual problems in multi-layer networks. Based on the examples, the advantages of the methodology are discussed in Section 8.

8 ADVANTAGES OF APPLYING THE METHODOLOGY TO AN ALL-IP NETWORK

The application of this methodology offers many advantages when applied to All-IP networks. The analysis of multi-layer network protection and alarming provides a detailed view of the protection and alarming as well as the relationship between them. Such a detailed view enables prioritization of faults for correction. By identifying the requirements for the protection strategies of different network layers, the network provider can establish the foundation of an end-to-end protection strategy.

Corresponding to the different types of failure events, the methodology details alarm-triggers, and lays out the alarms' traversal path through the different network layers. Thus another application of the methodology can help failure localization at the network level.



Legend:
AIS = Alarm Indication Signal
LOF = Loss of Frame
LOS = Loss of Signal
OTU =Optical Transport Unit
PRBS = Pseudo Random Bit Signal
SCTP = Stream Control Transmission Protocol

Figure 3 - Relationship of Protection & Alarming

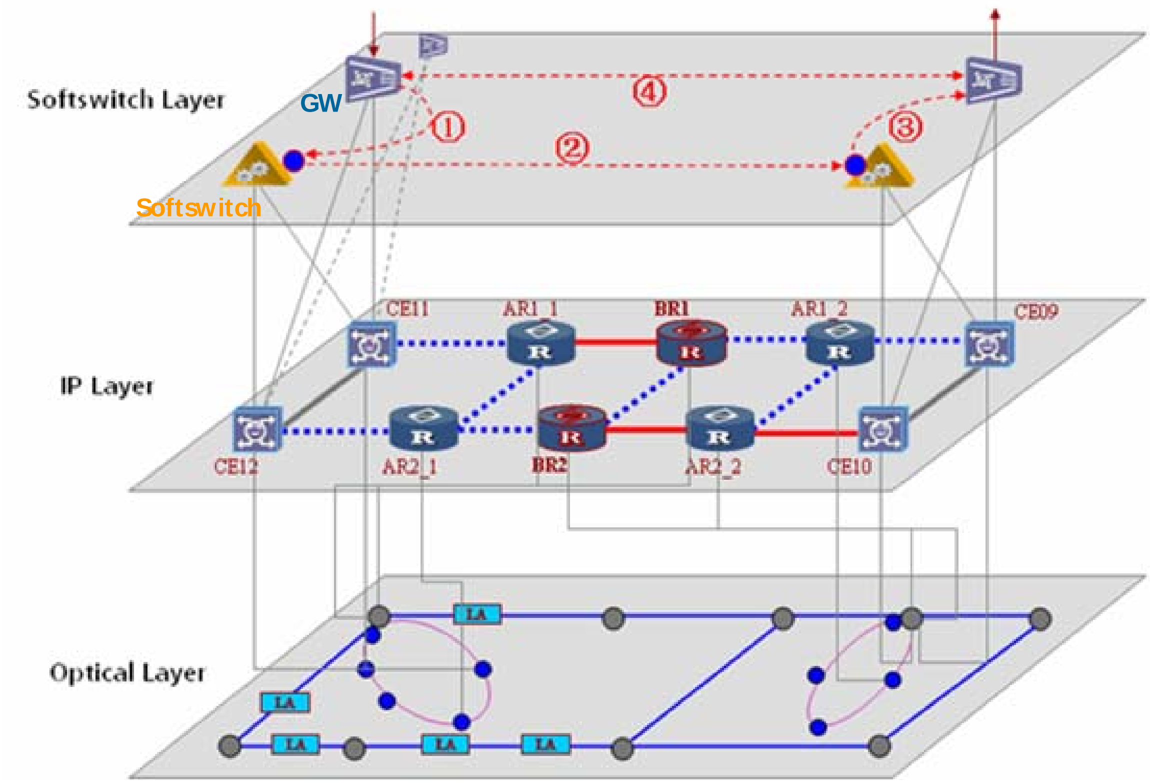
For illustrative purposes, Figure 3 shows some of the information available from a network FMEA analysis of a network comprising of three layers: the optical layer or the physical layer 1, the IP layer or layer 2 and layer 3, and the softswitch layer or the application layer. It is based on an example that corresponds to failures like the one discussed in the Example in Section 9 below. The figure shows the trigger conditions for the alarms, the subsequent escalation of alarms through the different layers, and the recovery actions that take place. The figure shows the results for two kinds of failures - Interruption and Degradation.

A degradation event will result in B1/B2/B3 alarm at the optical layer. If the failure is not fixed, then the increasing bit error rate will result in an SCTP link congestion alarm at the softswitch layer. The alarm-trigger settings where shown in Figure 3 are for example only. A network-operator will have to determine the values suitable to a specific network based on an understanding of the impact of failures on services.

Another benefit accruing from the above examples is the improvement of the alarm manuals. The alarm manuals assist operations in the identification of failures and in the location of faults to enable efficient handling of the identified problem. They contain details of flow of alarms through the different network-layers, and guidance for handling those alarms. Their effectiveness depends on incorporating best practices that will minimize the loss of service and limit the business impact on the service provider. The application of network FMEA enables detailed handling guidance for the many alarms of the various layers of the All-IP network (i.e., alarms for the optical transport network, alarms for the IP bearer network, and alarms for the softswitch network). The improved manuals include the effects and the possible causes of these alarms. Overall, more comprehensive guidance is provided to different groups responsible for the network operations**.**

9 USE CASE: APPLICATION OF THE METHODOLOGY TO AN ALL-IP NETWORK

We illustrate the above methodology with an example. Prior to performing the network FMEA methodology, it is necessary to have an understanding of the network and its requirements for the services it supports. This understanding leads to the characterization of unacceptable behavior -- i.e., failure. Part of this understanding will include a network diagram showing different layers of the network topology with the network elements in each layer and an overview of how they are connected. The FMEA can be developed around these logical relations. An example of such a diagram is shown in the Figure 4 below.



Legend:
CE = Customer Equipment
AR = Access Router
BR = Border router
LA = line Amplifier
GW = Gateway

Figure 4 - An Example Network to which the network FMEA methodology is applied

The network in this example comprises of three layers where the optical layer is equivalent to the physical layer 1, the IP layer is equivalent to layer 2 and layer 3, and the softswitch layer being equivalent to the application layer. The dotted arrows in the softswitch layer indicate that the Network Elements on both sides of the dotted arrows are not connected directly, but by an IP network. The dotted lines in the IP layer mean that the Network Elements at the ends are connected by an optical network. The connection between softswitch and Customer Equipment is Fast Ethernet, and the connection between Network Elements is Gigabit Ethernet.

9.1 Example: Fiber cut resulting from a cable dig-up

Cable dig-ups are a common cause of fiber-cuts and the resulting network failure. Work has been done on addressing this issue including tracking trends of such failures [Nrsc-1999], and the development of best practices [Nrsc-1993], [Nrsc-1996], and [Nrsc-1997]. After the root cause analyses of failures, steps to prevent their recurrence were documented in [Fcc-Nrc], [Nrsc-1996], and [Nrsc-1997].

Loss of service due to a cable cut can be prevented by the use of protection mechanisms. However, the network operators have to be careful in their choice of the different network-layer alarms and the alarm-triggers. This choice requires care to ensure there is multi-layer cooperation among the alarm-trigger settings.

The following is an example of a network FMEA for a cable dig-up. The steps and the figures described below follow the methodology illustrated by Figure 2 above. The flow of alarms is shown by Figure 3 above. The alarms and alarm-trigger settings in the example are for illustrative purposes only.

Failure Event: Fiber Cut

Failure Mode: Accidental dig-up by utility staff.

> Note: Due to past experience with such failures, this failure mode would be identified during design. However, it will benefit the design team to review information on similar failure events occurring in the field. Such information can point to particular nuances of a failure mode that will benefit the network FMEA.

Severity: A fiber cut failure, can potentially affect the network causing loss of services for a large number of customers. A common reason is the lack of correlation of the recovery mechanisms in the different layers of the networks. This lack of correlation can cause service down time to exceed acceptable levels.

Protection: Each layer will have its own protection mechanisms as shown below for this example. The design challenge is to ensure compatibility by appropriate choice of these protection mechanisms.

Optical Layer:

- Optical Line Protection
- Optical Channel Protection
- Optical Multiplex Section Protection,
- Automatic Protection Switching.

IP Layer: Route re-convergence following the Link Down alarm.

Softswitch Layer: Stream Control Transmission Protocol (SCTP) link switchover following the SCTP alarm.

Detection Alarms: Each layer will have its own detection alarms. The design challenge is to ensure compatibility by appropriate choice of the alarm-trigger settings. In this example, the alarms and their setting are the following:

Optical Layer Alarms:

- Loss of Signal (LoS);
- Loss of Frame (LoF); and
- Alarm Indication Signal (AIS).

IP Layer Alarms: Link Down alarm that is triggered following a delay exceeding 100 ms on the optical layer.

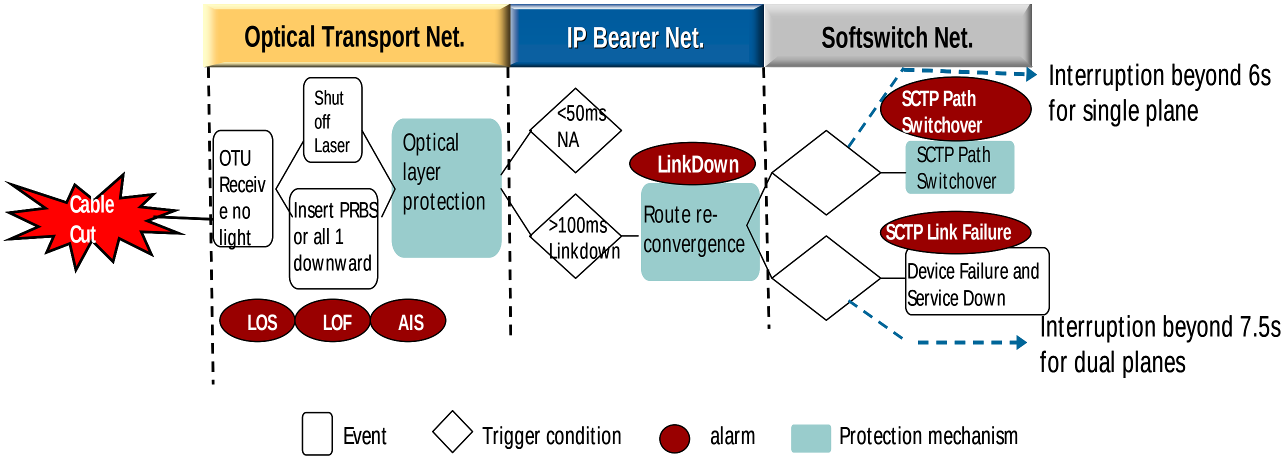
Softswitch Layer Alarms:

- SCTP Path Switchover alarm that is triggered following a delay exceeding 6s on a single softswitch plane.
- SCTP Link Failure alarm that is triggered following a delay exceeding 7.5s on the dual softswitch planes. Dual-plane is used in softswitch network for higher reliability. In the event a plane fails, the traffic on the plane can failover to the other plane.

Priority: This failure will have high priority. A fiber cut could potentially result in loss of service to a large number of customers.

Action & Follow-Up:

(i) Immediately fix the fiber cut by switching traffic to the protection fiber. Document detailed report of the incident.



Legend:
AIS = Alarm Indication Signal
LOF = Loss of Frame
LOS = Loss of Signal
OTU =Optical Transport Unit
PRBS = Pseudo Random Bit Signal
SCTP = Stream Control Transmission Protocol

Figure 5 - An Example of Alarm-Flow following a cable-cut in a multi-layer network

(ii) The alarms will escalate in time through the different layers of the network as shown in Figure 5, if the problem remains unsolved. To ensure coordination amongst the different layers in All-IP networks the hold-off timers shall be synchronized. Otherwise, in the event of a failure, this lack of coordination between the layers can lead to race conditions. Different network layers will resort to simultaneous restoration activity that lead to route flapping and network instability and other undesired behavior. Furthermore, prevent future incidents by adopting suitable best practices [Nrsc-1993], [Nrsc-1996], and [Nrsc-1997] and adopting steps to prevent their recurrence in [Fcc-Nrc], [Nrsc-1996], and [Nrsc-1997].